保安資訊--本周(台灣時間2022/01/14)賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，可保護包括財富500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 120 萬個受保護端點上總共阻止了 2.168 億次攻擊。這些攻擊中有 96% 在感染階段前就被有效阻止：**(2022/01/10)**

- 在**25萬2,700**台端點上，阻止了**1.185億**次嘗試掃描**Web**服務器的漏洞。
- 在**48萬9,200**台端點上，阻止了**4,130萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬4,200**台**Windows**伺服主機上，阻止了**2,790萬**次攻擊。
- 在**19萬5,300**端點上，阻止了**1,090萬**次嘗試掃描伺服器漏洞。
- 在**10萬8,400**台端點上，阻止了**540萬**次嘗試掃描在**CMS**漏洞。
- 在**15萬1,500**台端點上，阻止了**390萬**次嘗試利用的應用程式漏洞。
- 在**45萬3,600**台端點上，阻止了**1,330萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,600**台端點上，阻止了**410萬**次加密貨幣挖礦攻擊。
- 在**4萬6,900**台端點上，阻止了**480萬**次向惡意軟體**C&C**連線的嘗試。
- 在**9,200**台端點上，阻止了**20萬4,900**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

2022/01/13

Coinbase 用戶面臨網路釣魚活動激增的風險

隨著加密貨幣對世界的開放程度越來越高，加密貨幣的受歡迎程度不斷提高，現在主要經紀人之客戶成為覬覦的對象。最近幾週，試圖竊取 Coinbase（用於購買、出售、轉移和存儲加密貨幣的線上平台）用戶憑證的網路釣魚攻擊有所增加。這些行動幕後的黑手已經建立了多個虛假的 Coinbase 網站，其中許多網站使用一種被稱為域名仿冒的技術。賽門鐵克觀察到惡意電子郵件和簡訊都被用作初始感染媒介，如果成功引誘，會將用戶重新轉導向到這些虛假網站。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Malicious Phishing Site: Phishing Suspicious Request 2

賽門鐵克的端點防護行動裝置版本 (IOS/Android)：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一的 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊(SMS)網路釣魚攻擊。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱已於第一時間收錄於不安全分類列表中。

2022/01/13

OceanLotus (*海蓮花) 使用網頁封存檔散布後門

已觀察到 OceanLotus 組織（也稱為 APT32 或 SealLotus）使用 MHT 和 MHTML 等網頁封存檔來散布後門惡意軟體。該組織正試圖透過使用這些較不起眼的檔案類型來躲避檢測。初始感染媒介是一個 rar 壓縮檔案，其中包含網頁封存檔案，然後擴展具有惡意 VBA 巨集的 Office 文件，這些文件再利用後門感染系統。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1

2022/01/13

MuddyWater APT 組織對中東組織的網路攻擊

根據美國網路司令部最近的一份報告，被稱為 MuddyWater（又名 Seedworm）的 APT 組織一直在利用各種工具和技術在世界各地進行攻擊。MuddyWater 至少從 2017 年 2 月開始活躍，主要針對中東的組織，但也包括歐洲和北美的企業。據觀察，該組織將攻擊重點放在能源、政府和電信部門。該組織最近使用的工具包括 PowGoop 加載程序惡意軟體、Mori 後門、各種隧道和 JavaScript 工具。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/01/13

惡意垃圾郵件行動中的 RAT Nanocore、Netwire 和 AsyncRAT

2021 年 10 月，一個研究團隊發現一個惡意垃圾郵件行動，總共出現了三個遠端存取木馬(RAT)，分別名為 nanocore、netwire 和 asyncRAT。報告中的詳細資訊顯示，大多數受害者位於美國、義大利和新加坡。有人提到，攻擊者的 C&C 伺服器正在濫用 Microsoft Azure 和 Amazon Web Services 的雲端服務，以降低行動成本，並使防禦者更難追踪其運作。

帶有惡意 ZIP 附件的網路釣魚電子郵件將成為其初始攻擊媒介，在該壓縮檔中是包含惡意 JS、VBS 和批次檔腳本載入程式的 ISO 映像檔。載入程序將幫助建立 C&C 通信以獲取 RAT 有效籌載，目的是從受感染的機器或設備中竊取資料。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術 (Snoar) 的防護：

- SONAR.SuspDataRun
- SONAR.Zbot!gen8

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Infostealer
- ISB.Downloader!gen

- ISB.Downloader!gen52
- ISB.Downloader!gen53
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan.Gen.NPE
- Trojan Horse
- Trojan.Nancrat
- Trojan.Nancrat!g1
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Backdoor.Ratenjay.C/D Activity
- System Infected: JS.Downloader Activity 34
- System Infected: Netweird.B Activity 2
- System Infected: Trojan.Backdoor Activity 629
- System Infected: Trojan.Nancrat Activity 2
- System Infected: Trojan.Revetrat Activity 2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱已於第一時間收錄於不安全分類列表中。

2022/01/13

網路釣魚導致資料竊取--韓國知名入口網站也遭殃

韓國一家網際網路公司 Kakao Corp，最近遭受具有破壞憑證和提供惡意下載雙重功能的嚴重網路釣魚攻擊。如果用戶點擊電子郵件中的鏈接，他們將首先看到一個相似頁面，以引誘輸入他們的帳戶憑證。此時，如果用戶提供他們的憑證，則該帳戶將被盜用。

此外，如果用戶從該網路釣魚站瀏覽網頁，則會下載一個看起來像是來自另一個韓國入口網站：Naver 提供的保護工具。如果運行此程序，電腦將感染竊密惡意程式，該竊密惡意程式將長駐在電腦中，從系統和用戶操作中收集詳盡的資訊。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於行為偵測技術 (Snoar) 的防護：

- SONAR.SuspBeh!gen657

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/12

Kuzuluy 網路釣魚變種，鎖定 PayPal 憑證

網際網路上有無數可供公眾使用的網路釣魚工具包，並且多年來一直在進行純粹的網路釣魚活動。這種形式的網路犯罪很容易被吸收，以至於惡意投入者的數量比惡意軟體大得多。多年來，最令人垂涎的憑證之一是 PayPal。在最近一個例子中，據報導，在歐洲發現了一種名為 Kuzuluy 的舊網路釣魚工具包的變種。攻擊者試圖通過這些工具包生成的虛假 PayPal 網站來使受害者輸入其 PayPal 憑證。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱已於第一時間收錄於不安全分類列表中。

2022/01/12

TellYouThePass 被發現用 Golang 編寫用於跨平臺勒索

TellYouThePass 勒索軟體已被發現利用最近 Log4Shell 的漏洞做有效載荷。已部署的最新版本是用 Golang 編寫，並且已經觀察到 Windows 和 Linux 跨平臺變種。這個新版本還試圖透過其內部核心功能的隨機化來避免檢測和分析。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.Cryptlocker!g75

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE

2022/01/12

發現新型的多平臺後門 SysJoker

一種被稱為 SysJoker 的新型多平臺後門已經在網路上被觀察到。該惡意軟體針對 Windows、Linux 和 macOS 平臺偽裝成系統更新套件。一旦進入受感染的系統，SysJoker 將收到來自攻擊者的 C&C 伺服器的指令。根據那些資料，它可能會下載並執行其他惡意軟體有效載荷。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/12

Emotet 回歸提供更多惡意軟體

2021 年 12 月初，觀察到 Emotet 活動略有增加，早在同年 4 月，當局就查封了其基礎設施並取消了殭屍網路業務。在 12 月初的事件後，沒有看到隨後的攻擊。現在，惡意軟體作者透過啟動新的垃圾郵件活動並使用新 URL 格式和個人化的登錄頁面繼續他們的活動。Emotet 的感染可以為訊息竊取者、勒索軟體和特洛伊木馬打開大門。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.MSExcel!g4
- SONAR.MSExcel!g6

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.MalMacro!gen3
- Trojan.Mdropper
- WS.Malware.1
- WS.SecurityRisk.4

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱已於第一時間收錄於不安全分類列表中。

2022/01/12

潘朵拉的盒子破裂了—流竄的RAT

Pandora HVNC 是一款具有資訊竊取功能的遠端存取軟體，至少自 2021 年年中以來一直在銷售，最近有人已經設法破解並免費分享它。破解版本已經在不同的網站，論壇和社交媒體上得到了迴響，因此賽門鐵克一直在觀察越來越多利用此 RAT 的網路犯罪活動。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/01/11

Flubot 銀行惡意軟體，繼續發展和傳播

Android 銀行惡意軟體：Flubot，繼續困擾著世界各地的行動使用者。2021 年初在西班牙逮捕分支附屬機構並沒有遏止惡意軟體的發展，現在在威脅態勢下觀察到更新 5.2 版本。雖然整體攻擊鏈和惡意軟體功能保持不變，但最新版本在 DGA（動態網域產生演算法）和 C&C 通信方面有所改進。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

- Android.Reputation.1
- Android.Reputation.2

賽門鐵克的端點防護行動裝置版本(IOS/Android)還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 的重要來源之一的 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊(SMS)網路釣魚攻擊。

2022/01/11

Agent Tesla 在惡意軟體行動圈仍然大受歡迎

當今威脅態勢下，惡名昭彰且具有 RAT 功能的竊密惡意軟體：Agent Tesla，仍是駭客集團和個人中非常受歡迎的惡意軟體選項。賽門鐵克持續觀察世界各地不同複雜程度的活動。多年來，我們已經看到這種威脅透過不同的感染方法傳播，但惡意電子郵件仍然是最常用。通常使用普通社交工程（帳單、報價、運輸、SWIFT、備件等）來引誘受害者。

在最近的行動中觀察到的一些電子郵件主旨：

- استعلام خريد PUMP 8 X 6 X 14 SPARE PARTS MD-PUSP-2906-HM
- Payment Advice
- Your latest DHL invoice : BKKR005789102
- Confirmación de transferencia
- UPDATED STATEMENT OF ACCOUNT
- PAYMENT for pending invoices
- Statement Of Account
- Shipping Advice - 4081791001-1002 4084301001-1002, ETD 27 DEC. 2021

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.AM.E!g20
- SONAR.SuspBeh!gen93
- SONAR.SuspDataRun

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Atesla
- Scr.Malcode!gdn30

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/01/11

AvosLocker 勒索軟體增加了對Linux的支援，並攻擊了 VMware ESXi 機器

AvosLocker 是另一種勒索軟體變種，它增加對加密 Linux 系統的支援，據報導它一直針對 VMware ESXi 虛擬機。感染後，惡意軟體將嘗試終止 VMware 伺服器上任何虛擬機並啟動加密過程。加密完成後，惡意軟體會將 .avoslinux 副檔名附加到加密檔中，並投放支付贖金的說明。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.RansomAvos
- Trojan Horse

2022/01/10

SFile 勒索軟體出現 Linux 平台的變種

SFile 勒索軟體（也稱為 Escal）攻擊於 2020 年 2 月首次出現，初始版本僅適用於 Windows 系統。然而，去年年底的調查證實，SFile 惡意軟體現在也在 Linux 環境中運行。Linux 變種的運行方式與 Windows 版本幾乎相同，但有一些明顯的改進。在過去幾年中，該集團以針對企業和政府網路而聞名，其中包括幾家中國公司。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan Horse

2022/01/10

非同質化代幣/不可替代代幣(NFT:non-fungible token)的社交工程和加密錢包劫持

最近幾個月，全球似乎已經陷入不可替代代幣（NFT：non-fungible token）的狂熱，這種與區塊鏈相關的業務繼續呈指數型增加。基本上，NFT 是存儲在區塊鏈上唯一且不可分拆的資料單元。它們可以採用數位藝術的形式，包括照片、影片和聲音。

在網際網路上，全球趨勢的任何東西通常都會迅速被用作社交工程誘餌，試圖吸引受害者，最終導致惡意軟體或網路釣魚企圖。如所預料那樣，賽門鐵克觀察到一個垃圾郵件行動，其中參與者正在利用 NFT 來分發惡意軟體，這些惡意軟體將用他們的加密位址替換原 NFT 加密錢包中的位址。

感染指標：

- 郵件主旨:NFT_John_jones.exe
- 檔案名稱:NFT_John_jones.exe

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn30
- Trojan Horse
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/01/10

RedLine (*紅線) 資訊竊取程式，利用 Omicron 疫情的恐慌誘人上鉤

最近觀察到與 RedLine (*紅線) 資訊竊取變種程式散布相關的活動。攻擊者利用 Omicron 疫情上升的恐慌，來進行社交工程行動以散布此惡意軟體。RedLine 惡意軟體用於從受入侵電腦中洩露大量資訊，例如：系統資訊、登錄帳戶密碼等資訊、網頁資訊 Cookie 和 VPN 憑證。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/10

一個惡意程式 Formbook 行動：烏茲別克的請求

Formbook 是一個知名的資訊竊取抓取器，已經存在多年，它仍然是威脅環境中頂級的竊密程式。該惡意軟體正被多個團體和個人使用，賽門鐵克繼續透過不同的社交工程技術觀察全球範圍內的活動。

例如：一位參與者最近將自己偽裝成烏茲別克一家知名化學公司，並向全球各地的公司發

送電子郵件，重點是中東、南亞和東歐--電子郵件主旨：The Uzbekistan request (烏茲別克請求)。

利用這種威脅大多數活躍參與者主要使用電子郵件作為初始媒介，其中包含舊的和較新的 Microsoft Office 漏洞，作為其投放 Formbook 的一種方式。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Exp.CVE-2017-11882!g5
- Trojan Horse
- Scr.Malcode!gdn30
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/01/10

由 Patchwork APT 發佈的 Ragnatela RAT

印度駭客組織 Patchwork，散布遠端存取木馬 Ragnatela（義大利文中的「蜘蛛網」）。

根據最近發佈的一份報告，Patchwork APT 組織一直利用魚叉式網路釣魚活動，透過惡意 RTF 檔案積極散布稱為 Ragnatela 的 BADNEWS RAT 新變種。Ragnatela RAT 包括各種功能，允許攻擊者在遠端電腦上執行任意命令、擷取螢幕截圖、記錄擊按鍵，上傳檔案或下載並執行其他有效籌載。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Bloodhound.RTF.10
- Trojan Horse
- Trojan.Mdropper

基於機器學習的防禦技術：

- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/01/09

PirateStealer 資料竊取程式及其變種，專門敲詐 Discord VOIP 用戶

Discord 是一個成功的 VOIP 平台，被包括全球遊戲玩家和串流影音用戶在內的許多人使用。多年來，它的受歡迎一直吸引著網路犯罪，我們看到大量的網路釣魚嘗試和新的資訊竊賊，目的在竊取 Discord 的用戶憑證。最近幾個月，又一個出現在網站、社交媒體和流行的軟體開發和版本控制平台上。這種被稱為“PirateStealer”開放原始碼惡意軟體，專門用於竊取 Discord 用戶資訊和接管帳戶。由於公開可用，這種威脅已經被不同的團體和個人使用。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Suspicious.Epi.3
- Trojan.Gen.NPE
- Trojan.Pirasteal
- Ws.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/01/07

Night Sky (*夜空) 勒索軟體，在年底壓軸登場

截至 2021 年 12 月下旬，已觀察到一種新發現名為 Night Sky (*夜空) 勒索軟體。Night Sky 執行典型的檔案加密，還包括先行盜竊資料。然後，勒索軟體使用雙重勒索戰術來施壓受害者支付贖金以進行檔案解密，並避免被盜資料公諸於世。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Nightsky
- Trojan.Gen.2
- WS.Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g3

2022/01/06

IcedID (Bokbot) ，分派紅隊演練工具Cobalt Strike

TA551也稱為“Shathak”，以發動針對英語系受害者的惡意電子郵件之惡意軟體攻擊行動而聞名。最近報導顯示該組織再次引人注目，但這次是使用德語和意大利語系樣板的 Word 檔案。

感染慣例包括使用從惡意 Word 檔案中提取的 DLL 安裝 IcedID (Bokbot)，隨後不久將 Cobalt Strike Beacon 訊號發送器作為用於後續攻擊的附加惡意軟體。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- SONAR.IcedID!g1
- WS.Malware.1
- W97M.Downloader

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。